



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/566,584	01/31/2006	Stephan Blicker	BLICKER1	3683
1444	7590	04/14/2009	EXAMINER	
BROWDY AND NEIMARK, P.L.L.C.			SIMS, JING F	
624 NINTH STREET, NW				
SUITE 300			ART UNIT	PAPER NUMBER
WASHINGTON, DC 20001-5303			2437	
			MAIL DATE	DELIVERY MODE
			04/14/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/566,584	BLICKER ET AL.	
	Examiner	Art Unit	
	JING SIMS	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 17 February 2009.
- 2a) This action is **FINAL**. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-18 is/are pending in the application.
- 4a) Of the above claim(s) 11 is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-10, and 12-18 is/are rejected.
- 7) Claim(s) 16 is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ . |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ . | 6) <input type="checkbox"/> Other: _____ . |

DETAILED ACTION

1. This action is responsive to communications: application 10/566,584 filed on 1/31/2006; amendment filed on 2/17/2009.
2. Applicant's arguments, with respect to claims 1-10, and 12-15 have been fully considered but they are not persuasive.

Claim Objections

3. Claim 16 is objected to because of the following informalities: "the check-in ID is one of an mobile station ISDN Number and an International Mobile Subscriber Identity IMSI" (lines 1-2), and "the pre-recorded ID is one of the subscriber's MSISDN and IMSI pre-recorded in a subscriber database" (line 3), according to the specification page 3, lines 13, and 16, it should be "the check-in ID is one of an mobile station ISDN Number and/or an International Mobile Subscriber Identity IMSI" and "the pre-recorded ID is one of the subscriber's MSISDN or IMSI pre-recorded in a subscriber database".

Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1, 3, 4, 16 and 18 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claims 1, 3, 4, 16 and 18, the limitation "check-in ID" renders these claims are as vague and indefinite. It is not clear to the examiner whether applicants refer to "user ID" "IP address" "PrivID" or "MSISDN"; therefore, applicants might consider amending claim 1 to read.

Claims 2, 5-15, 17 are rejected under 35 U.S.C. 112, second paragraph. Claims 2, 5-15, 17 are directly or in-directly dependent on claim 1, therefore, Claims 2, 5-15, 17 inherent the deficiency of the claim 1.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1, 3-5, 9-12, 14 are rejected under 35 U.S.C. 102(b) as being anticipated by Skog et al. (US 6977917) (hereinafter Skog).

As per claim 1, Skog discloses "*a method for transparent access authentication of subscribers connected to an authenticating network domain by a General Packet Radio Service GPRS core network or an Universal Mobile Telecommunication System*

UMTS network, comprising" (col. 2, lines 25-29, associating a mobile terminal's temporarily assigned IP with a MSISDN number for use with authentication within a service network. Skog discloses the service network is a GPRS network in col. 5, lines 43-45); "*receiving a context creation request from a subscriber*" (col. 4, lines 28-31, the mobile terminal transmits a message to the access server in order to establish a connection); "*assigning an IP address to the context*" (col. 3, lines 63-65, the mapping session database includes a plurality of storage locations for an assigned temporary IP address and an associated MSISDN of the mobile terminal; also in col. 4, lines 54-57, the IP address is dynamically allocated to the mobile terminal by the access server or the RADIUS server during the connection setup); "*receiving a check-in ID from the subscriber*" (col. 4, lines 33-35, the mobile terminal transmits authentication information including the user ID); "*receiving a private identification PrivID from the subscriber, the PrivID is being correlated with a pre-recorded ID of the subscriber in a subscriber database*" (col. 5, lines 6-12, the MSISDN of the mobile terminal is determined by the associated IP address, therefore, the correlation of MSISDN and IP has been disclosed; Skog discloses the pre-recorded ID as the IP address and the MSISDN are stored as record with in a database in col. 4, lines 62-64); "*and authenticating the subscriber by comparing the check-in ID with the pre-recorded ID, and indicating authentication when the check-in ID matches the pre-recorded ID*" (col. 4, lines 60-62, and col. 5, lines 1-3, the WAP gateway as an accounting are able to map the IP address and the MSISDN and establish the connection).

As per claim 3, Skog discloses “*the method according to claim 1, further comprising: using a Gateway GPRS Support Node to receive the context creation request*” (fig. 2, reference numbers 50 and 60; and col. 3, lines 35-38, the RADIUS Accounting server sends back an acknowledgment that the Accounting Start packet has been received. Since Skog discloses the access server can be implemented in GGSN (GPRS Gateway Serving Node), then the Accounting Start packet can be received by using GPRS Gateway Serving Node); “*querying the context request to a Radius server*” (col. 3, lines 63-65, the mapping session database includes a plurality of storage locations for an assigned temporary IP address and an associated MSISDN of the mobile terminal); “*using the Radius server to receive the check-in ID*” (col. 4, lines 1-6, RADIUS accounting messages is to be delivered to RADIUS Accounting server. The information in the packet includes MSISDN number and the IP address of the mobile terminal etc); “*and storing the IP address and the check-in ID in a session database*” (col. 4, lines 4-6, the information within a packet of relating to IP address and MSISDN number is used to update the database).

As per claim 4, Skog discloses “*the method according to claim 1, further comprising: a proxy server to compare the check-in ID with the pre-recorded ID, wherein the subscriber database is an application domain database*” (col. 5, lines 6-12, the WAP gateway determine the IP address of the mobile terminal by examining the IP packet header. The MSISDN of the mobile terminal is determined by examining the mapping session database and the associated IP address).

As per claim 5, “*the method according to claim 1, further comprising: using a Radius server to compare a subscriber's IP address in an IP network layer with the assigned IP address*” (col. 5, lines 6-9, the WAP gateway may determine the IP address of the mobile terminal by examining the IP packet header to determine the IP address of the mobile terminal).

As per claim 7, Skog discloses “*the method according to claim 1, comprising the steps of, in all subsequent messages arriving at the proxy server (5), checking for a match of IP address in the IP packet overhead field for source address with that in the application layer protocol header fields and verifying the matching pairs against the IP address assigned by the Radius server (2)*” (col. 5, lines 1-9, once the connection is established, the WAP gateway may determine the IP address of the mobile terminal by examining the IP packet header to determine the IP address of the mobile terminal).

As per claim 9, Skog discloses “*a system of units in a mobile telecommunication network, comprising: characterised at least a first authentication unit connected to a session database via a first data line*” (Fig. 2, RADIUS Server in MSC/VLR; and col. 4, 31-36, mobile terminal requests a access to access server 60, the access server using a password authentication procedure to authenticate the mobile terminal. Since user transmits its user ID and password to access server, there must be a database related to access server for user ID and password information included in the request to be authenticated); *a second unit connected to the session database via a second data line; wherein the second unit assembles data according to the method of claim 1*” (Fig. 2, RADIUS accounting server 75 and DB 118; col. 4, lines 58-64, the WAP gateway as an

accounting request message to enable mapping between identifiers. The IP address and the MSISDN are stored as a record).

As per claim 10, Skog discloses “*the system of units according to claim 9, wherein the first authentication unit comprises a registration server*” ((Fig. 2, RADIUS Server in MSC/VLR. The RADIUS Server/access server appears to be a registration server).

As per claim 12, Skog discloses “*the system of units according to claim 9, wherein the second unit comprises a proxy server*” (col. 5, lines 6-9, the WAP gateway may determine the IP address of the mobile terminal 45 by examining the IP packet header to determine the IP address of the mobile terminal. It describes the functionality of proxy servers. Also in col. 1, lines 54-59, Skog implies the proxy server has been implemented within WAP network).

As per claim 14, Skog discloses “*the system of units according to claim 13, wherein the second unit is connected to a subscriber database*)” (Fig. 5, the authentication unit is connected to Users DB which includes the information of subscriber).

As per claim 16, Skog discloses “*the method of claim 1, wherein the check-in ID is one of an Mobile Station ISDN Number MSISDN and an International Mobile Subscriber Identity IMSI received from the subscriber*” (col. 4, lines 58-62, the MSISDN of the mobile terminal are transmitted over the PPP connection from the access server to the WAP gateway), “*and the pre-recorded ID is one of the subscriber's MSISDN and*

IMSI pre-recorded in a subscriber database” (col. 4, lines 62-64, the IP address and MSISDN are stored as a record within the mapping session database).

As per claim 17, Skog discloses “*the system according to claim 12, wherein the proxy server (5) is connected to a subscriber database (4)* ” (col. 5, lines 6-12, the WAP gateway determine the IP address of the mobile terminal by examining the IP packet header. The MSISDN of the mobile terminal is determined by examining the mapping session database and the associated IP address).

As per claim 18, Skog discloses “*a method for transparent access authentication of subscribers connected to an authenticating network domain by a General Packet Radio Service GPRS core network or an Universal Mobile Telecommunication System UMTS network*” (col. 2, lines 25-29, associating a mobile terminal’s temporarily assigned IP with a MSISDN number for use with authentication within a service network. Skog discloses the service network is a GPRS network in col. 5, lines 43-45), “*using data assembled by a network layer during establishment of a PDP context in GPRS networks, comprising*” (col. 5, lines 6-9, the gateway may determine the IP address of mobile terminal by examining the IP packet header to determine the IP address of the mobile terminal): “*receiving, at a Gateway GPRS Support Node, a context creation request from a subscriber*” (col. 4, lines 28-31, the mobile terminal transmits a message to the access server in order to establish a connection; col. 5, in a GPRS network, the access server would be implemented in GGSN GPRS Gateway Serving Node), “*the Gateway GPRS Support Node, in response to the receipt of the context creation request, querying a registration server to get an IP address assigned*

for the context” (col. 3, lines 63-65, the mapping session database includes a plurality of storage locations for an assigned temporary IP address of the mobile terminal); “*within the context, receiving at the registration server, a check-in ID from the subscriber; storing, for each PDP context, a pair of an IP address and the check-in ID in a session database*” (col. 4, lines the IP address and the MSISDN are stored as a record within the mapping session database within the gateway); “*checking, in a proxy server, the check-in ID from a registration server session database and a pre-recorded ID stored in an application domain database, for a match*” (col. 4, lines 31-36, Mobile terminal transmits authentication information including user ID to access server using a password authentication procedure PAP. For being able to comparing the user ID, a pre-recorded user ID must be in a database), “*if the check-in ID matches the pre-recorded ID, checking, in the proxy server, a subscribers IP address assigned in the IP network layer for a match with the IP address assigned by the registration server, and using a proxy server to parse an application layer for IP addresses given in headers of registration messages and to compare the IP addresses with the network layer IP address for a match*” (col. 5, lines 1-12, if the connection is established, the WAP gateway may determine the IP address of mobile terminal by examining the IP packet header to determine the IP address of the mobile terminal; the MSISDN if determined by examining the mapping session database and the associated IP address), “*wherein the IP address given in the headers was already checked for a match with the IP address assigned by the registration server*” (col. 3. lines 63-65, the mapping session

database includes a plurality of storage locations for an assigned temporary IP address.
Since the IP is pre-assigned, therefore it has been checked).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. **Claim 2** is rejected under 35 U.S.C. 103(a) as being unpatentable over Skog in view of Chaudhary et al. (US 7155526) (hereinafter Chaudhary).

As per claim 2, Skog discloses *claim 1*. Skog does not specifically disclose the “*wherein the step of authenticating the subscriber includes an A3/A8 algorithm based on an end devices SIM card*”.

However, Chaudhary discloses it as verifying user equipment by sending RAND to SIM card and get a response generated by the GSM algorithm A8 and then establish PDP context message to GGSN over GTP control protocol (col. 11, lines 36-48, col. 12, lines 11-19, and Figure 5).

Skog and Chaudhary are analogous art because they are from the same field of endeavor of wireless network authentication.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify sending account message to RADIUS server via data packets from a user as discussed in Skog by indicating the packets are in PDP context data and the

authentication method is A8 algorithm as described by Chaudhary, because it would provide for the purpose of deploying a standard authentication algorithm such as A8, since standard algorithms are broadly developed, tested and deployed and consequently makes the system developments easier and more efficient (col. 11, lines 36-48, col. 12, lines 11-19, and Figure 5).

10. Claims 6, 13, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Skog in view of Pirttimaa et al. (US 0154400 A1) (hereinafter Pirttimaa).

As per claim 6, Skog discloses “*wherein the IP address given in the headers was already checked for a match with the assigned IP address*” (col. 4, lines 51-54, after the connection is established between the access server and the mobile terminal, the only information included in the IP packets that been transmitted is the IP address. Since the IP is the IP address has been assigned to, there is a match for the IP); however, Skog does not explicitly disclose “*using a proxy server to parse an application layer for IP addresses given in headers of registration messages and to compare with the assigned IP address for a match*”.

Pirttimaa discloses it as comparing the source address, since the source address indicated in the SIP message corresponds to a “true” source address, e.g. the actual source address of the IP datagram indicated by the stored at the P-CSCF (page 3, [0043]). Since the source address has been extracted from the SIP message, the parsing process must be taken in place. The SIP message indicates the parsing is in an application layer.

Skog and Pirttimaa are analogous art because they are from the same field of endeavor of wireless network authentication.

It would have been obvious to one of ordinary skill in the art at the time to modify the authentication process of matching application layer IP address as discussed in Skog, and add the detail description of a proxy server parses IP address from application layer as described by Pirttimaa because it would provide the purpose of offering the complete details about how the process has been accomplished (page 3, paragraph 00420).

As per claim 13, Skog only discloses claim 9, but not the rest of the claim. Pirttimaa discloses "*the system of units according to claim 9, wherein the second unit comprises a proxy server connected to a Proxy Call State Control Function via a routing module*" (Fig. 3, modules 31 and 33; Fig. 4, modules 31 and 33; page 3, [0043], lines 1-9, based on the result of the address comparison, the P-CSCF makes a forwarding decision. If the compared IP address indicates the same location no fraudulent attack can be assumed. The IP comparison and forward the data packets to P-CSCF unit implies the existence of proxy server and the routing module).

As per claim 15, Pirttimaa discloses "*the system of units according to claim 13, wherein a routing module selects messages from one of the proxy server and the Proxy Call State Control Function by evaluating the PrivID*" (page 3, lines 1-4, based on the result of the address comparison. The address appears to be a user/attacker's private ID).

11. **Claim 8** is rejected under 35 U.S.C. 103(a) as being unpatentable over Skog in view of Naim et al. (US 6678517 B2) (hereinafter Naim).

As per claim 8, Skog discloses *the method according to claim 1*; however, Skog does discloses "*wherein a routing module (7) is provided which is a standard entry point for all messages and wherein the routing module (7) decides by evaluation of the PrivID which network node will handle the message*".

Naim discloses it as Wireless Soft Switch (WSS) acts as a standard entry point handling wireless calls for 2G, 2.5G and 3G mobile phones. WSS has an SIP interface. SIP is a signaling protocol used to handle signaling message (column 3, line 26-37, Figure 1 and Figure 2(a), Figure 1). In the instant application, PrivID is the requested information given by subscriber during registration for the service. PrivID and SIP both include message that can be identified by an entry point, then make a transferring decision based on.

Skog and Naim are analogous art because they are from the same field of endeavor of to authenticate to a wireless network.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the GGSN entry point as discussed in Skog by adding WSS entry point as described in Naim because it would provide the accessing ability for 2G, 2.5G or 3G wireless networks (column 3, line 26-37, Figure 1 and Figure 2(a)).

Response to Arguments

1. Applicant's request for reconsideration of the 35 U.S.C. § 112, first paragraph rejection to the disclosure of "a first authentication unit" and "a second unit" of the last Office action is persuasive and, therefore, the 35 U.S.C. § 112, first paragraph rejection is withdrawn.
2. Applicant's request for reconsideration of the 35 U.S.C. § 112, first paragraph rejection to the connection between routing module (7) in claim 15 and registration server(2) claim 10 of the last Office action is persuasive and, therefore, the 35 U.S.C. § 112, first paragraph rejection is withdrawn.
3. One page 15, lines 12-13, the applicants argue that Skog does not disclose that matching the MSISDN from the mobile terminal 155 with the MSISDN from the user database during the authentication procedure in original claim 4. Since applicants removed this limitation from the claim(s), the argument is moot; however, examiner still would like to point out Skog discloses "matching the MSISDN from the mobile terminal 155 with the MSISDN from the user database during the authentication procedure" (col. 5, lines 6-12, the MSISDN of the mobile terminal is determined by examining the mapping session database during the authentication process for the mobile terminal's request to contact the WAP applications).
4. On page 15, lines 16-21, the applicants argue that Skog discloses the IP address and MSISDN information in the session database is updated during the authentication procedure, not prerecorded information before the authentication procedure. Examiner respectfully disagrees. Skog discloses the authentication process in several steps. For example, the password authentication procedure (col. 4, line 36), then the

authentication steps for the mobile terminal to access WAP application (col. 5, line 13). The IP address and MSISDN are stored as a record in session database (col. 4, lines 62-64) is the preparation step for authenticating the mobile terminal to WAP application (col. 5, lines 6-12); therefore, to update the session database is to pre-recording the IP and MSISDN before the authentication starts.

5. On page 16, lines 4-6, the applicants argue that "the mail server 180 uses the MSISDN as a label in searching information of the user parameters, not to compare the MSISDN from the session database to authenticate the user". Since applicants cancelled the limitation that described above, the argument is moot. Please refer to the rejection to the amended claims 4 and 1 that listed under rejection section 102 above.

6. On page 16, lines 7-9, the applicants argue that Skog fail to disclose "authenticating the subscriber by comparing the check-in ID with the pre-recorded ID for match" which recited in the amended independent claim 1. For the response please refer to the reject to claim 1 that listed under rejection section 102 above.

Conclusion

8. **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JING SIMS whose telephone number is (571)270-7315. The examiner can normally be reached on 7:30am-5:00pm EST, Mon-Thu.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jing Sims

/J. S./

Application/Control Number: 10/566,584
Art Unit: 2437

Page 17

Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437